Policies and Procedures
POLICY: User Authorization
Policy #4
Effective Date: April 2, 2014

Purpose: This policy describes the duty of the ILHIE Authority and Participant to define the requirements for establishing user access controls and other technical safeguards to ensure user authorization.

Policy: The ILHIE Authority shall grant Participants access to the ILHIE as set forth in these Policies and Procedures and the Data Sharing Agreement. Access rights shall be based on individual roles and job responsibilities.

1.0 Access Controls. Consistent with the Permitted Purposes, the ILHIE Authority and Participants shall implement technical policies and procedures to allow ILHIE access only to those Authorized Users or software programs that have been granted access rights.

1.1 The ILHIE Authority shall implement and communicate to Participants specific role classifications to which a Participant may assign Authorized Users and the specific System permissions associated with each such classification.

1.2 Each Participant shall appoint a System Administrator. Each Participant may also appoint one or more alternate System Administrator(s). Each System Administrator must submit to an authentication and verification process as required by the ILHIE Authority in order to be granted access to the ILHIE. After successfully completing the verification process, the System Administration may create, manage, and terminate Authorized Users under the Participant's account as set forth by the ILHIE Authority.

1.3 Each Participant's System Administrator may create, manage, and revoke access to the ILHIE for its Authorized Users under the Participant's account, including through log-in/password generation and resetting in accordance with these Policies and Procedures.

1.4 The ILHIE Authority and each Participant shall provide Authorized User access only to its respective Workforce, contractors, Subcontractors and agents who have a need to request, use, or disclose Protected Health Information through the ILHIE for a Permitted Purpose.

1.5 Participants are responsible for initially creating, managing, and revoking Authorized Users in accordance with these Policies and Procedures, the Data Sharing Agreement, and Applicable Law.

2.0 Authorized Users. The ILHIE Authority and Participant shall use reasonable care in selecting its respective Authorized Users and shall require that the Authorized Users act in compliance with these Policies and Procedures, the Data Sharing Agreement, and Applicable Law.

2.1. Participant shall have a valid and enforceable agreement with each of its Authorized Users that require the Authorized User to, at a minimum:

(i) Comply with these Policies and Procedures, the Data Sharing Agreement, and Applicable Law, as applciable;
(ii) Reasonably cooperate with the ILHIE Authority and Participant on issues related to these Policies and Procedures;
(iii) Request, use, or disclose Protected Health Information only for a Permitted Purpose;
(iv) Use proprietary information or Protected Health Information received from an Other Participant in accordance with these Policies and Procedures;
(v) As soon as reasonably practicable after determining that a Breach occurred, report such Breach to the Participant or if Authorized User cannot report the Breach to Participant then report the Breach to the ILHIE Authority; and
(vi) Refrain from disclosing to any other person any passwords or other security measures issued to the Authorized User by the Particpant.

Notwithstanding the foregoing, for Authorized Users who are employed by a Participant or who have agreements with the Participant which became effective prior to the effective date of the Participant's Data Sharing Agreement, compliance with this Section may be satisfied through written policies and procedures that address (i) through (vi) so long as the Participant can document that there is a written requirement that the Authorized User must comply with the Policies and Procedures.

3.0 Access Revocation and Reinstatement. Participant shall comply and require its Authorized Users to comply with the ILHIE access suspension, revocation, and reinstatement Policies and Procedures as set forth in the Sanctions Policy (Policy #15).

4.0 Breach. Participant shall comply and require its Authorized Users to comply with the Breach Notification and Mitigation Policy (Policy #21) in the event of a Breach or suspected Breach.

5.0 Training. All members of the ILHIE Authority and each Participant's respective Workforce, and their respective contractors, Subcontractors or agents, as applicable, who will have access to the ILHIE as an Authorized User, shall undergo both initial and ongoing security awareness training, to ensure compliance these Policies and Procedures, the Data Sharing Agreement, and Applicable Law.

5.1. No Workforce member, contractor, Subcontractor or agent shall be provided with access to the ILHIE, an unique identifier or a password prior to completing training.

6.0 Compliance. Participant shall comply with these Policies and Procedures. The ILHIE Authority will monitor and enforce compliance with and adherence to these Policies and Procedures.

6.1 Participant shall cooperate with the ILHIE Authority in its monitoring and enforcement of the Participant's compliance with these Policies and Procedures.

Associated Policies and References:
45 C.F.R §164.308(a)(5)(i)
45 C.F.R §164.306(d)
Data Sharing Agreement
Access Use and Disclosure of Protected Health Information
Breach Notification and Mitigation
Enforcement
Sanctions
User Authentication

Definitions
Applicable Law
Authorized User
Participant
Protected Health Information
System Administrator
Workforce